TOP-LEVEL RADIOLOGICAL, NUCLEAR, AND PROCESS SAFETY STANDARDS AND PRINCIPLES FOR TWRS PRIVATIZATION CONTRACTORS

U.S. Department of Energy
Richland Operations Office

DOE/RL-96-0006
Revision 1
July 1998

Preface

As noted below, the DOE regulatory approach for the radiological, nuclear, and process safety regulation of the TWRS Privatization Contractor is described in an integrated set of four documents, which should be read in the order listed below to obtain an understanding of the regulatory approach. The DOE regulatory approach to radiological, nuclear, and process safety clearly places on the Contractor the responsibility to achieve adequate safety, comply with applicable laws and legal requirements, and conform to top-level safety standards and principles stipulated by DOE. According to a prescribed process, DOE interacts with each Contractor in arriving at DOE decisions to approve and authorize Contractor activities. The DOE maintains a continuing interaction with the Contractor to ensure that the Contractor is meeting the safety conditions of its contract and the conditions of the DOE approvals; is complying with applicable laws and legal requirements; and is conforming to the DOE-stipulated top-level safety standards and principles.

Consistent with applicable laws and legal requirements, the requirements applied to each Contractor are tailored to control the hazards specific to the activities of that Contractor. With knowledge and understanding of the hazards specific to its activities, each Contractor is required to identify and recommend for DOE approval a set of safety standards to which the Contractor certifies, that when properly implemented, will ensure for that Contractor's activities 1) adequate safety, 2) compliance with applicable laws and legal requirements, and 3) conformance to DOE-stipulated top-level safety standards and principles. When DOE approves the set of Contractor-recommended safety standards, the set together with the DOE-stipulated top-level safety standards and principles becomes the requirements which are applied to the Contractor's activities.

The four documents that describe the DOE regulatory approach for the radiological, nuclear, and process safety regulation of TWRS Privatization Contractors are:

1. *Concept of the DOE Regulatory Process for Radiological, Nuclear, and Process Safety for TWRS Privatization Contractors*, DOE/RL-96-0005; Revision 0,

2. *DOE Regulatory Process for Radiological, Nuclear, and Process Safety for TWRS Privatization Contractors*, DOE/RL-96-0003; Revision 0,

3. *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006; Revision 0, and

4. *Process for Establishing a Set of Radiological, Nuclear, and Process Safety Standards and Requirements for TWRS Privatization*, DOE/RL-96-0004; Revision 0.

Table of Contents

List of Tables

1.0 Introduction

1.1 Purpose

This document provides a set of top-level radiological, nuclear, and process safety standards and principles prescribed by the U. S. Department of Energy (DOE) for accomplishing the expected level of safety for TWRS Privatization. Use of these top-level standards and principles does not provide a blanket waiver to safety regulations that apply to DOE activities, rather they are an additional consideration, stipulated by DOE, for the identification of the Contractor's radiological, nuclear, and process safety standards and requirements. The Contractor shall employ the top-level radiological, nuclear standards and principles in two ways. First, the Contractor must address these top-level standards and principles in the standards and requirements identified and recommended by the Contractor. Second, the Contractor shall incorporate the top-level radiological, nuclear, and process standards and principles into the recommended standards and requirements.

The top-level radiological, nuclear, and process safety standards and principles in this document are independent of the Contractor's waste processing technology and associated facility design. The standards provided in this document are high-level statements that express DOE's expectations for the performance of safety-related activities associated with facility design, construction, pre-operational testing, operation, and deactivation. The safety principles provided in this document are a set of broad statements of ways to achieve the expected level of safety, which represent international experience and perspectives. With due consideration for the hazards related to TWRS Privatization activities, the principles were derived from a number of sources, including the International Atomic Energy Agency's *Basic Safety Principles for Nuclear Power Plants* (International Nuclear Safety Advisory Group 75-INSAG-3); DOE Orders and Regulations; DOE Directives, the Code of Federal Regulations governing the Nuclear Regulatory Commission's (NRC) regulation of commercial nuclear facilities and operations), Center for Chemical Process Safety, *Guidelines for Technical Management of Chemical Process Safety*, OSHA Regulations and recent programs for which comparable high-level safety requirements were formulated. In recognition of the safety practices unique to process safety, process safety principles stipulated by DOE are presented as a separate set. The Contractor is expected achieve efficiency through the elements common to radiological and nuclear safety, and process safety. Radiological and nuclear safety objectives also are included to provide goals for the Contractor to assess the adequacy of radiological and nuclear safety.

1.2 Scope

This document shall be used for the identification and recommendation of radiological, nuclear, and process safety standards and requirements. This document and the standards and requirements apply only to the radiological, nuclear, and process safety regulation of the Contractor during Phase I of TWRS Privatization. While the scope of the regulation is predominantly limited to the Contractor's activities from initial design through deactivation, it also must include the Contractor's consideration of site characteristics, its use of site services, and its coordination with the DOE/RL's integrated emergency response.

2.0 Radiological and Nuclear Safety Standards

The radiological and nuclear standards in this section are the human dose standards to which all facility activities of the Contractor involving radiological and nuclear hazards must comply. These standards are consistent with radiological exposure limits embodied in DOE and NRC regulations and the perspectives of the International Council on Radiological Protection. The standards presented herein do not include standards for various release pathways and are not necessarily a complete set for human doses. The absence of other standards is not intended to exempt the Contractor from the obligation to comply with all applicable requirements pertaining to limiting exposures to workers and the public.

2.1 Individual

The top-level radiological and nuclear safety standards for workers, co-located workers, and the public for various situations are listed in Table 1. Footnotes to the table refer to the origin of a specific standard. Additional information on terminology, definitions, and methods can be found in those references. As noted in the references, some of the standards can not be applied independent of other dose contributors located on the Hanford Site.

Table 1. Dose[1] Standards Above Normal Background

Description	Estimated Probability of Occurrence $P(yr^{-1})$	General Guidelines	Worker	Co-located Worker	Public
Normal Events: Events that occur regularly in the course of facility operation (e.g., normal facility operations).	P=1	Normal modes of operating facility systems should provide adequate protection of health and safety.	≤5 rem/yr [2] ≤50 rem/yr any organ, skin, or extremity [2] ≤15 rem/yr lens of eye [2] ≤1.0 rem/yr ALARA design objective[3]	≤5 rem/yr[3] 1.0 rem/yr ALARA design objective[3]	≤10 mrem/yr (airborne pathway)[4] ≤100 mrem/yr (all sources)[5] ≤100 mrem/yr[6] ≤25 mrem/yr[7]
Anticipated Events: Events of moderate frequency that may occur once or more during the life of a facility (e.g., minor incidents and upsets).	$10^{-2}<P<1$	The facility should be capable of returning to operation without extensive corrective action or repair.	≤5 rem/event[8] ≤1.0 rem/event ALARA design objective[3]	≤5 rem/event[8] ≤1.0 rem/event ALARA design objective[3]	≤100 mrem/event[8]
Unlikely Events: Events that are not expected, but may occur during the lifetime of a facility (e.g., more severe incidents).	$10^{-4}<P\leq 10^{-2}$	The facility should be capable of returning to operation following potentially extensive corrective action or repair, as necessary.	To be derived[9]	To be derived[9]	≤5 rem/event[10]

Table 1. Dose[1] Standards Above Normal Background (continued)

Description	Estimated Probability of Occurrence $P(yr^{-1})$	General Guidelines	Worker	Co-located Worker	Public
Extremely Unlikely Events[11]: Events that are not expected to occur during the life of the facility but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material.	$10^{-6} < P \leq 10^{-4}$	Facility damage may preclude returning to operation.	To be derived[9]	To be derived[9]	≤ 25 rem/event[12] ≤ 300 rem/event to thyroid[12]

1 Dose is assumed to be the committed effective dose equivalent from inhaled radionuclides and any direct radiation from the accident
2 10 CFR 835.202 Occupational exposure limits for general employees and 10 CFR 20.1201 Occupational dose limits for adults
3 10 CFR 835.1002(b) Facility design and modification
4 Proposed Rule 10 CFR 834.102(2) Airborne emissions only, all DOE sources of radionuclides (60 FR 47498, Federal Register, 9/13/95) and 40 CFR 61.92 Public dose from emissions of radionuclides to the ambient air from DOE facilities
5 Proposed Rule 10 CFR 834.101 Public primary dose limit (60 FR 47498, Federal Register, 9/13/95) and 10 CFR 20.1301(a)(1) Dose limits for individual members of the public
6 10 CFR 835.206 Limits of members of the public entering a controlled area and 10 CFR 20.1301(b) Dose limits for individual members of the public
7 Proposed Rule 10 CFR 834.221 Public primary dose limit for radioactive waste (60 FR 47498, Federal Register, 9/13/95)
8 Proposed Rule 10 CFR 60 Disposal of high-level radioactive waste in geologic repositories; design basis events (60 FR 15180, Federal Register, 3/22/95)
9 Specific limits to be derived and proposed by the Contractor. Examples of such derived limits and implementation approaches are described in the DOE/EH report *Methods for the Assessment of Worker Safety Under Radiological Accident Conditions at Department of Energy Nuclear Facilities*, EH-12-94-01, June 1994. Specific limits will be finalized as part of the standards identification and approval activities to be performed early in Part A of the program.
10 10 CFR 72.106 Control area of an independent spent fuel storage installation or monitored retrievable storage facility
11 They represent the upper bounds on failures or accidents with the probability of occurrence sufficiently high to require consideration in the design.
12 10 CFR 100.10 Siting evaluation factors

3.0 Radiological and Nuclear Safety Objectives

The safety objectives included in this section are radiological and nuclear safety goals, which if accomplished, should ensure protection of public and worker health and safety. The Contractor should use these objectives to determine 1) the effectiveness in achieving the expected level of safety and 2) the need for additional measures.

3.1 General Safety Objectives

3.1.1 Operations Risk Goal

The risk, to the population (public and workers) in the area of the Contractor's facility, of cancer fatalities that might result from facility operation should not exceed one-tenth of one percent (0.1%) of the sum of cancer fatality risks to which members of the U.S. population generally are exposed.[13]

3.1.2 Accident Risk Goal

The risk, to an average individual in the vicinity of the Contractor's facility, of prompt fatalities that might result from an accident should not exceed one-tenth of one percent (0.1%) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population generally are exposed.[14]

3.1.3 Worker Accident Risk Goal

The risk, to workers in the vicinity of the Contractor's facility, of fatality from radiological exposure that might result from an accident should not be a significant contributor to the overall occupational risk of fatality to workers.[15]

3.2 Radiation Protection Objective

Ensure that during normal operation radiation exposure within the facility and radiation exposure and environmental impact due to any release of radioactive material from the facility is kept as low as is reasonably achievable (ALARA) and within prescribed limits, and ensure mitigation of the extent of radiation exposure and environmental impact due to accidents.

3.3 Technical Safety Objectives

3.3.1 Public Protection

Measures in the design and operation of the facility to protect the public against accident conditions should be evaluated against acceptable guidelines to demonstrate that they perform their intended purpose with high confidence.

3.3.2 Worker Protection

Measures in the design and operation of the facility to protect the workers against accident conditions should be evaluated using an acceptable approach to demonstrate that they perform their intended purpose with high confidence.

3.3.3 Accident Vulnerability Mitigation

Particular care should be taken to identify, evaluate, and prevent and/or mitigate any vulnerabilities to accidents that might, by themselves, result in a release of radioactive material that exceeds acceptable levels.

---

[13] For evaluation purposes, individuals are assumed to be located within 10 miles of the controlled area.
[14] For evaluation purposes, individuals are assumed to be located within one mile of the controlled area.
[15] For evaluation purposes, workers are assumed to be located within the controlled area.

4.0 General Radiological and Nuclear Safety Principles

The safety principles presented in this section are fundamental ways to achieve safety, which by experience, have proven to be effective and have become the basis for accepted radiological and nuclear safety practice. Although the experience base for these principles comes largely from the commercial nuclear reactor community, these principles have merit for any nuclear facility. In facilities with hazards much reduced from those of nuclear reactors, measures to accomplish these principles may be less extensive and require less complex approaches than those related to reactor safety. These principles shall be addressed in the standards and requirements identified and recommended by the Contractor.

4.1 Overall Principles

4.1.1 Defense in Depth

4.1.1.1 Defense in Depth

To compensate for potential human and mechanical failures, a defense-in-depth strategy should be applied to the facility commensurate with the hazards such that assured safety is vested in multiple, independent safety provisions, no one of which is to be relied upon excessively to protect the public, the workers, or the environment. This strategy should be applied to the design and operation of the facility.

4.1.1.2 Prevention

Principle emphasis should be placed on the primary means of achieving safety, which is the prevention of accidents, particularly any that could cause an unacceptable release.

4.1.1.3 Control

Normal operation, including anticipated operational occurrences, maintenance, and testing, should be controlled so that facility and system variables remain within their operating ranges and the frequency of demands placed on structures, systems, and components important to safety is small.

4.1.1.4 Mitigation

The facility should be designed to retain the radioactive material through a conservatively designed confinement system for the entire range of events considered in the design basis. The confinement system should protect the workplace and the environment.

4.1.1.5 Automatic Systems

Automatic systems should be provided that would place and maintain the facility in a safe state and limit the potential spread of radioactive materials when operating conditions exceed predetermined safety setpoints.

4.1.1.6 Human Aspects

The human aspects of defense in depth should include a design for human factors, a quality assurance program, administrative controls, internal safety reviews, operating limits (Technical Safety Requirements), worker qualification and training, and the establishment of a safety/quality program.

4.1.2 Safety Responsibility

4.1.2.1 Safety Responsibility

Ultimate responsibility for the safety of the facility rests with the Contractor. In no way should this responsibility be diluted by the separate activities and responsibilities of designers, suppliers, constructors, the Regulatory Unit, or independent oversight bodies.

4.1.2.2 Safety Assignments

The assignment and subdivision of responsibility for safety should be kept well defined throughout the life of the facility.

4.1.2.3 Site and Technical Support

The Contractor should assure commitments from relevant parties to provide data and services needed to fulfill its safety commitments.

4.1.2.4 Operating Experience and Safety Research

Operating experience and the results of research relevant to safety should be obtained, reviewed, and analyzed, and lessons that are learned should be implemented in the design, construction or modification, and operation of the facility.

4.1.3 Authorization Basis

4.1.3.1 Authorization Basis

Material that is part of the authorization basis should be established, documented, and submitted to the Director of the Regulatory Unit for evaluation and in support of decisions and regulatory oversight. The Contractor should maintain the material current with respect to changes made to the facility design and administrative controls and in the light of significantly new safety information.

4.1.4 Safety/Quality Culture

4.1.4.1 Safety/Quality Culture

A safety/quality program should be established that governs the Contractor's actions and interactions of all personnel and organizations engaged in activities related to the facility and emphasizes excellence in all activities. The Contractor should have safety and quality responsibilities specifically identified in its operations.

4.1.5 Configuration Management

4.1.5.1 Formal Configuration Management

Formal configuration management should be applied to all facility activities during the program's lifetime to ensure that programmatic objectives related to radiological, nuclear, and process safety are fully achieved. Work should be performed and controlled according to pre-approved plans and procedures that clearly delineate responsibilities. Documented records should be retained.

4.1.5.2 Contractor Design Knowledge

The Contractor operating organizations should become and remain familiar with the features and limitations of components included in the design of the facility. They should obtain appropriate input from the design organization on pre-operational testing, operating procedures, and the planning and conduct of training.

4.1.5.3 Design Documentation

A system should be used to control and maintain accurate as-built drawings during the life of the facility related to radiological, nuclear, and process safety.

4.1.6 Quality Assurance

4.1.6.1 Quality Assurance Application

Quality assurance and quality control should be applied throughout all phases and to all activities associated with the facility as part of a comprehensive system to ensure with high confidence that all items delivered and services and tasks performed meet required standards.

4.1.6.2 Established Techniques and Procedures

The Contractor should use well proven and established techniques and procedures supported by quality assurance practices to provide high quality equipment and achieve high quality construction.

4.1.6.3 Operational Quality Assurance Programs

Operational quality assurance and control programs should be established by the Contractor to assist in ensuring satisfactory performance in facility activities important to safety.

4.2 Design, Construction, and Pre-Operational Testing

4.2.1 Design

4.2.1.1 Safety Design

The facility should be designed for a set of events such as: normal operation, including anticipated operational occurrences, maintenance, and testing; external events; and postulated accidents.

4.2.1.2 Risk Assessment

Acceptable risk analyses should be applied during the design to delineate provisions for the prevention and mitigation, including emergency preparedness and response, of otherwise risk-dominant events.

4.2.1.3 Safety Analysis

A safety analysis should be carried out as required to evaluate the safety performance of the design and identify requirements for operations.

4.2.2 Proven Engineering Practices/Margins

4.2.2.1 Proven Engineering Practices

Safety technologies incorporated into the facility design should have been proven by experience or testing and should be reflected in approved codes and standards. Significant new design features should be introduced only after thorough research and model or prototype testing at the component, system, or facility level, as appropriate.

4.2.2.2 Common-Mode/Common-Cause Failure

Design provisions should be included to limit the loss of safety functions due to damage to several structures, systems, or components important to safety resulting from a common-cause or common-mode failure.

4.2.2.3 Safety System Design and Qualification

Structures, systems, and components important to safety should be designed and qualified to function as intended in the environments associated with the events for which they are intended to respond. The effects of aging on normal and abnormal functioning should be considered in design and qualification.

4.2.2.4 Codes and Standards

Codes and standards for vessels and piping should be supplemented by additional measures (such as erosion/corrosion programs and piping in-service inspections) to mitigate conditions arising that could lead to an unacceptable release of radioactivity during the operational life of the facility.

4.2.2.5 Criticality

The facility should be designed and operated in a manner that prevents nuclear criticality.

4.2.3 Radiation Protection

4.2.3.1 Radiation Protection Practices

An acceptable system of radiation protection practices should be followed in the design, construction, and pre-operational testing phases of the facility for the protection of workers and the public.

4.2.3.2 Radiation Protection Features

At the design stage, radiation protection features should be incorporated to protect workers from radiation exposure and to keep emissions of radioactive effluents ALARA and within prescribed limits.

4.2.3.3 Deactivation, Decontamination, and Decommissioning Design

The design of the facility should incorporate provisions to facilitate deactivation and the final decommissioning. The objective of these provisions should be to reduce radiation exposures to Hanford Site personnel and the public both during and following deactivation and decommissioning activities and to minimize the quantity of radioactive waste generated during deactivation, decontamination and decommissioning.

4.2.4 Emergency Preparedness

4.2.4.1 Support Facilities

The facility design should provide additional capability to place and maintain the facility in a safe state following an accident if the normal control areas are expected to become uninhabitable.

4.2.5 Inherent/Passive Safety Characteristics

Design features that enhance safety through simplified, inherent, passive, or other highly reliable means to accomplish safety functions should be employed to the maximum extent practicable.

4.2.6 Human Factors

4.2.6.1 Human Error

The possibility of human error in facility operations should be taken into account in the design by facilitating correct decisions by operators and inhibiting wrong decisions and by providing means for detecting and correcting or compensating for error.

4.2.6.2 Instrumentation and Control Design

Sufficient instrumentation and control capability should be provided so that under normal operating and postulated accident conditions the operators can diagnose facility conditions, place and maintain the facility in a safe state, and mitigate accidents. If necessary, measures should be provided to protect the operator in the performance of these functions.

4.2.6.3 Safety Status

Parameters to be monitored in the control room should be selected and their displays should be arranged to ensure that operators have clear and unambiguous indications of the status of facility conditions important to safety, especially for the purpose of identifying and diagnosing the actuation and operation of a system or components important to safety.

4.2.7 Reliability, Availability, Maintainability, and Inspectability (RAMI)

4.2.7.1 Reliability

Reliability targets should be assigned to structures, systems, and components or functions important to safety. The targets should be consistent with the roles of the structures, systems, and components or functions in different accident conditions. Provision should be made for appropriate testing and inspection of structures, systems, and components for which reliability targets have been set.

4.2.7.2 Availability, Maintainability, and Inspectability

Structures, systems and components important to safety should be designated, designed and constructed for appropriate inspection, testing, and maintenance throughout their operating lives to verify their continued acceptability for service with an adequate safety margin.

4.2.8 Pre-Operational Testing

4.2.8.1 Testing Program

A pre-operational testing program should be established and followed to demonstrate that the entire facility, especially items important to safety, have been constructed and function according to the design intent, and to ensure that weaknesses are detected and corrected.

4.2.8.2 Operational Systems and Functional Testing Procedures Validation

Procedures for normal facility and systems operation and for functional tests to be performed during the operating phase should be validated as part of the pre-operational testing program.

4.2.8.3 Safety Systems Data

During pre-operational testing, detailed diagnostic data should be collected on systems and components important to safety and the initial operating parameters of the systems and components should be recorded.

4.2.8.4 Design Operating Characteristics

During the pre-operational testing program, the as-built operating characteristics of process systems, and systems and components important to safety should be determined and documented. Operating points should be adjusted to conform to values in the design basis. Training procedures and limiting conditions for operation should be modified to accurately reflect the operating characteristics of the systems and components as built.

4.3 Operation

4.3.1 Conduct of Operations

4.3.1.1 Organizational Structure

The Contractor should exert full responsibility for the safe operation of the facility through a strong, unambiguous organizational structure.

4.3.1.2 Normal Operations

Operations should be conducted in accordance with approved technical safety requirements and in strict accordance with administrative and procedural controls.

4.3.1.3 Emergency Operating Procedures

To provide a basis for suitable operator response to accident conditions, emergency operating procedures should be established, documented and approved.

4.3.1.4 Readiness

The facility manager should ensure that all elements for safe facility operation are in place, including an adequate number of qualified and experienced workers. Minimum requirements also should be set for the availability of staff and equipment.

4.3.1.5 Internal Surveillance and Audits

Internal safety review procedures should be used by the Contractor to provide a continuing surveillance and audit of facility operational safety and to support the facility manager in overall safety responsibilities.

4.3.1.6 Operations Within the Authorization Basis

Operations should be conducted in accordance with approved TSRs. Limiting conditions of operation, limiting control settings, and safety limits should be established as necessary to ensure operation within the authorization basis.

4.3.1.7 Access to Technical Safety Support

Throughout the life of the facility, the Contractor should have access to engineering and technical support personnel, who are competent in all disciplines important to safety.

4.3.1.8 Operational Events

Facility management should institute measures to ensure that events relevant to safety are detected and evaluated, and that necessary corrective measures are taken promptly and information on them is disseminated. Operational event reports should be prepared and submitted to the Director of the Regulatory Unit. The facility management should have access to operational safety experience from other related facilities.

4.3.2 Radiation Protection

4.3.2.1 Radiation Practices

An acceptable system of radiation protection practices should be followed in the operational phase for the protection of workers and public.

4.3.2.2 Procedures and Monitoring

The radiation protection staffs of the Contractor's operating organizations should establish written procedures for the control, guidance, and protection of personnel; and routinely monitor facility site radiological conditions; the exposure of facility personnel to radiation; and releases of radioactive effluents.

4.3.2.3 Final Deactivation Plans and Provisions

Deactivation of the facility should be planned. These plans and provisions should incorporate radiation protection practices to protect Hanford Site personnel and the public, both during and following deactivation activities, and waste minimization procedures to reduce the amount of radioactive waste generated during deactivation.

4.3.3 Emergency Preparedness

4.3.3.1 Offsite Measures

Hanford Site and offsite mitigation measures should be provided to substantially reduce the effects of an unacceptable accidental release of radioactive material.

4.3.3.2 Accident Management Strategy

The results of analyses of the response of the facility to accidents with the potential for releases resulting in doses in excess of Environmental Protection Agency and the State of Washington emergency clean-up standards, beyond the facility control perimeter (security fence) should be used in preparing guidance on an accident management strategy.

4.3.3.3 Establishment and Continued Exercise of Emergency Plans

Emergency plans should be prepared before the startup of the facility, and should be exercised periodically to ensure that protection measures can be implemented in the event of an accident that results in, or has the potential for, unacceptable releases of radioactive materials within and beyond the facility control perimeter. Emergency planning zones defined around the facility should allow for the use of a graded response.

4.3.4 Training and Qualifications

4.3.4.1 Personnel Training

Personnel engaged in activities bearing on facility safety should be trained and qualified to perform their duties.

4.3.4.2 Training Programs

Programs should be established for continual training of operations and maintenance personnel to enable them to perform their duties safely and efficiently.

4.3.4.3 Conditions Beyond Design Basis

Operating staff should be trained and retrained in the procedures to follow if conditions exceed the design basis of the facility.

4.3.5 Operational Testing, Inspection, and Maintenance

4.3.5.1 Operational Testing, Inspection, and Maintenance

Structures, systems, and components important to safety should be the subject of appropriate, regular preventive maintenance, inspection, and testing and servicing when needed, to ensure that they remain capable of meeting their design requirements throughout the life of the facility. Such activities should be carried out in accordance with written procedures supported by quality assurance measures.

4.3.6 Security

4.3.6.1 Security

Adequate provisions for facility security and physical protection of structures, systems, and components important to safety should be provided.

4.4 Internal Safety Oversight

4.4.1 Safety Review Organization

The Contractor should establish a framework for its safety review organizations that are responsible for assuring the safety of the facility. The separation between the responsibilities of the safety review organizations and those of the other organizations should remain clear so that the safety review organizations retain their independence as safety authorities.

4.4.2 Qualified Personnel

Internal safety oversight should be conducted by qualified personnel to ensure that the safety standards are consistently met.

4.4.3 Recommendation for Initiation of Construction

The Contractor should request authorization for construction only after being satisfied by appropriate internal assessments that the main safety issues have been satisfactorily resolved and that the remainder are amenable to solution before operations are scheduled to begin.

4.4.4 Unresolved Safety Questions

All facility modifications after operations begin that can affect safety should be assessed by the Contractor for an "unreviewed safety question" and positive determinations submitted to the Director of the Regulatory Unit for review.

5.0 General Process Safety Principles

The safety principles presented in this section are fundamental ways to achieve process safety, which have been proven to be effective in the chemical industry and have become the basis for accepted process safety practice. These principles shall be used to address all process hazards associated with the Contractors' facilities. These principles shall be addressed by the Contractor in the standards identified in the Safety Requirements Document . The standards and the controls implementing these standards should be tailored to the significance of the hazard.

5.1 Overall Principles

5.1.1 Process Safety Management

The Contractor should use a comprehensive process safety management program to eliminate or reduce the incidence, or mitigate the consequences of accidental hazardous chemical releases, process fires, and process explosions. This program should address management practices, technologies, and procedures.

5.1.2 Process Safety Objective

Process safety management should confirm that the facility is properly designed, the integrity of the design is maintained, and the facility is operated according to the safe manner intended.

5.1.3 Process Safety Responsibility

The ultimate responsibility for process safety rests with the Contractor. In no way should this responsibility be diluted by the separate activities and responsibilities of designers, suppliers, constructors, the Regulatory Unit, or independent oversight bodies.

5.2 Process Safety Management Program

5.2.1 Process Safety Information

The Contractor should develop and maintain certain important information about the process. This information is intended to provide a foundation for identifying and understanding the process hazards. The process safety information includes, but is not limited to, a summary of material data, a description of each process and its operation, and equipment design data.

The information should confirm that the equipment is appropriate for the operation, that its integrity is maintained, and that it meets appropriate codes and standards.

5.2.2 Process Hazard Analysis

The Contractor should perform a process hazards analysis using acceptable industry practices. The process hazards analysis should be appropriate for the complexity of the process and the hazard. The Contractor should consider the effects of engineering and administrative controls, human factors, facility siting, and previous incidents in the hazard analysis. The Contractor should document the results of the hazards analysis including process hazards and possible safety and health effects. The Contractor should submit the results of the hazards analysis to the Director of the Regulatory Unit for evaluation and in support of authorization decisions and regulatory oversight.

One of the purposes of the hazard analysis is to evaluate the adequacy of the design and operating procedures. The Contractor should establish a system to address the findings in order to assure that the equipment and procedures provide an adequate degree of protection against accidents.

The Contractor should review and update the hazard analysis periodically to assure that the process hazards analysis is consistent with the current process.

5.2.3 Operating Procedures

The Contractor should develop and implement written operating procedures that provide clear instruction for

safely conducting activities consistent with the process safety information. The procedures should address at least the following elements: steps for each operating phase of the process, operating limits, safety and health considerations, and safety systems and their functions.

5.2.4 Training

Each operator should be trained in an overview of the process and in the operating procedures. The training should include emphasis on the specific safety and health hazards, operating limits, emergency operations, and safety work practices. The employees should receive refresher training at an appropriate frequency considering the applicable standards and the nature of the hazards.

5.2.5 Subcontractors

The Contractor may engage a subcontractor to perform maintenance, renovations, or specialty work on, or adjacent to, the process. The Contractor should inform the subcontractor of potential hazards related to the subcontractor's work and take appropriate measures to ensure the subcontractors provide their workers with appropriate procedures and training necessary for performing their jobs safely.

5.2.6 Pre-startup Safety Review

The Contractor should perform a pre-startup safety review for the facility. Pre-startup reviews also should be performed prior to restarting the process after significant modifications have been made to the facility. The pre-startup review should confirm that prior to the introduction of hazardous materials that construction and equipment is in accordance with design specifications; safety operating, maintenance, and emergency procedures are in place; an adequate process hazards evaluation has been performed and the recommendations resolved; and training of employees has been completed. The results of this review should be submitted to the Director of the Regulatory Unit for evaluation and in support of authorization decisions and regulatory oversight.

5.2.7 Mechanical Integrity

The Contractor should implement a mechanical integrity program that includes written procedures, training for maintenance activities, inspection and performance testing of process equipment, and quality assurance measures. The program should include measures to correct deficiencies in equipment that are outside acceptable limits.

Note: A mechanical integrity program is a major and necessary element in a process safety management program because of its importance in ensuring equipment integrity, eliminating potential ignition sources, and for determining that equipment is designed, installed, and operating properly.

5.2.8 Hot Work Control

The Contractor should control hot work operations performed in or near the process or facility in order to ensure appropriate safety precautions, including fire prevention and protection, are taken prior to the work.

5.2.9 Management of Change

The Contractor should evaluate all planned changes involving the technology of the process and the facility design and operation in order to ensure that the impact on safety is analyzed and acceptable and to determine the need for modifications to operating procedures. The Contractor should establish and implement written procedures to manage changes to process chemicals, technology, equipment, and procedures; and changes to facilities. These procedures should address the technical basis for the proposed changes, impact of the changes on process safety, modification of the operating procedures, the schedule for proposed changes, and authorization for proposed changes.

5.2.10 Incident Investigation

The Contractor should investigate each incident which results in, or could reasonably have resulted in, a major accident. The investigation should be conducted promptly and appropriate corrective measures should be recommended and implemented. The results of the investigation should be submitted to the Director of the Regulatory Unit for evaluation and in support of regulatory oversight.

5.2.11 Emergency Planning and Response

The Contractor should establish and implement an emergency action plan in accordance with the applicable standards.

5.2.12 Compliance Audits

The Contractor should conduct a compliance audit periodically to certify that the procedures and practices developed under the process safety management program are adequate and are being followed. The frequency of compliance audits is based on the applicable standards and the nature of the process hazards. The Contractor should promptly determine and document an appropriate response to each finding of the compliance audit. The results of the audits should be available to the Director of the Regulatory Unit in support of regulatory oversight.

6.0 Glossary[16]

Acceptable Release. The release of radioactive material, within acceptable limits, to the environment.

Anticipated Operational Occurrences. Conditions of normal operation expected to occur one or more times during the life of the facility and include, but are not limited to, loss of off-site power to the process activity within the facility.

Authorization Agreement. The document mutually agreed upon by the Director of the Regulatory Unit and a regulated Contractor that specifies authorization terms and conditions.

Authorization Basis. The composite of information provided by a Contractor in response to radiological, nuclear, and process safety requirements that is the basis on which the Director of the Regulatory Unit grants permission to perform regulated activities.

Back-fit. The addition, elimination, or modification of 1) structures, systems, or components of the facility or 2) procedures or organizations required to operate the facility after the construction authorization has been issued.

Catastrophic Release. A major uncontrolled emission, fire, or explosion involving one or more highly hazardous chemicals that presents serious danger to employees in the workplace.

Co-located Worker. An individual within the Hanford Site, beyond the Contractor-controlled area, performing work for or in conjunction with DOE or utilizing other Hanford Site facilities.

Common-Cause Failures. Dependent failures that are caused by a condition external to a system or set of components that make system or multiple component failures more probable than multiple independent failures.

Common-Mode Failures. Dependent failures caused by susceptibilities inherent in certain systems or components that make their failures more probable than multiple independent failures due to those components having the same design or design conditions that would result in the same level of degradation.

Contractor(s). The private company(ies) selected to contract with DOE for construction and operation of the technologies and facilities necessary to retrieve, process tank waste, and deliver treated waste products to DOE for storage or disposal.

Contractor Representative (CR). The top manager of the Contractor Organization that has direct responsibility, accountability, and authority for performing the TWRS Privatization work subject to the set of standards.

Contractor-recommended set of standards and requirements. Those standards and requirements identified through a DOE-specified process and recommended by the Contractor Representative as necessary assurance that work will be performed in a manner that protects the workers, the public, and the environment from the actual hazards identified for the Contractor's specific work activities. (Also see the definition for "Requirements.") The recommended set serves as a basis for DOE review and approval by the Director of the Regulatory Unit, and the Contractor's issuance of the Safety Requirements Document.

Control Strategy. A set of generally described provisions (barriers, dilution/dispersal, physical limitations on material quantities, administrative material controls, confinement, ventilation of flammable gas, etc.) and/or approaches (defense in depth, use of passive features, prevention, mitigation, etc.) which are intended to ensure adequate control of a specific hazard and associated accidents in the context of the work.

Controlled Area. The physical area enclosing the facility by a common perimeter (security fence). Access to this area can be controlled by the Contractor. The controlled area may include identified restricted areas.

Deactivation Safety Evaluation Report. The document approved and issued by the Director of the Regulatory Unit that addresses the adequacy of the authorization basis for deactivation.

---

[16] Certain terms used in this document and listed in this glossary have origins in radiological and nuclear safety. Extension of their use to process safety may be useful but is not stipulated herein. It is expected that the extension of their use to process safety will be considered as part of the standards and requirements identification process.

Defense in Depth. The fundamental principle underlying the safety technology of the facility centered on several levels of protection including successive barriers preventing the release of radioactive materials to the workplace or environment. Human aspects of defense in depth are considered to protect the integrity of the barriers, such as quality assurance, administrative controls, safety reviews, operating limits, personnel qualification and training, and safety program. Design provisions, including both those for normal facility systems and those for systems important to safety help to: 1) prevent undue challenges to the integrity of the physical barriers; 2) prevent failure of a barrier if it is challenged; 3) where it exists, prevent consequential damage to multiple barriers in series; and 4) mitigate the consequences of accidents. Defense in depth helps to assure that two basic safety functions (controlling the process flow and confining the radioactive material) are preserved and that radioactive materials do not reach the worker, public, or the environment.

Design Basis. The information that identifies the specific functions to be performed by structures, systems, or components of the facility and the specific values or ranges of values chosen for controlling parameters as reference bounds for design.

Design-Basis Events. Postulated events providing bounding conditions for establishing the performance requirements of structures, systems, and components that are necessary to: 1) ensure the integrity of the safety boundaries protecting the worker; 2) place and maintain the facility in a safe state indefinitely; or 3) prevent or mitigate the event consequences so that the radiological exposures to the general public or the workers would not exceed appropriate limits. The Design-Basis Events also establish the performance requirements of the structures, systems and components whose failure under Design-Basis Event conditions could adversely affect any of the above functions.

Director of the Regulatory Unit (DRU). An individual who has been delegated the authority to execute the radiological, nuclear, and process safety regulation of TWRS Privatization Contractors.

DOE-Customer. A DOE employee who has knowledge of the equipment, facilities, and processes necessary for performance by the Contractor of the work activities to deliver the contracted services.

ESH Standards Experts (ESE). Individuals with knowledge and expertise relevant to the radiological, nuclear, or process standards and requirements in a particular environment, safety, and health discipline.

Facility. Those buildings and equipment directed to a common purpose and those activities and supporting elements occurring at a single location.

Final Safety Evaluation Report. The document approved and issued by the Director of the Regulatory Unit that addresses the adequacy of the authorization basis for operation.

Hazard. A source of danger (i.e., material, energy source, or operation) with the potential to cause illness, injury, or death to personnel, damage to an operation, or to the environment (without regard for the likelihood or credibility of accident scenarios or consequence mitigation).

Hazards Assessment Experts (HAE). Individuals with the knowledge, skills and abilities to identify, based on examination of the work activities defined, the hazards associated with the work activities, as well as the risk to the workers, public and environment attributable to those hazards.

Hazards Control Experts (HCE). Individuals with knowledge, skills and abilities to identify, based on examination of the work activities and associated hazards, the controls necessary to mitigate the hazards to an acceptable level.

Highly Hazardous Chemical. A substance possessing toxic, reactive, flammable, or explosive properties as defined by 29 CFR 1910.119.

Important to Safety. Structures, systems, and components that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological, nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation).

This definition includes not only those structures, systems, and components that perform safety functions and traditionally have been classified as safety class, safety-related or safety-grade, but also those that place frequent demands on or

adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems, or components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear, and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of important to safety, i.e., safety-related may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems, and components should be considered for inclusion within this definition.

Independent Oversight. Authorized oversight by bodies or groups having no financial, programmatic, or other direct interest in the activities or organizations under review and which are totally free of management relationships with those activities or organizations.

Independent Oversight Bodies. Independent Oversight Bodies are those established organizations that have no financial, programmatic, or other direct interest in and are outside the management structure of the Contractor and the Regulatory Unit. The independent oversight bodies include personnel qualified and skilled to critique, evaluate, and recommend that the regulatory oversight provided by the Regulatory Unit of the Contractor is effective.

Independent Review Team (IRT). A group of individuals with the appropriate knowledge and expertise to review the recommended standards set for completeness, credibility, and adequacy before the standards are recommended by the Contractor Representative to the Director of the Regulatory Unit.

Initial Safety Evaluation Report. The document, approved and issued by the Director of the Regulatory Unit, that addresses the capability or potential for obtaining future authorizations for construction, operation, and deactivation.

Integrated Safety Management Plan (ISMP) Evaluation Report. The document, approved and issued by the Director of the Regulatory Unit, that addresses the adequacy of the Contractor's Integrated Safety Management Program as reflected in its Integrated Safety Management Plan.

Integrated Safety Management Program. A set of integrated activities that is directed toward the management or control of radiological, nuclear, and process hazards such that adequate protection is provided to workers, the public, and the environment.

Limiting Conditions for Operations (LCO). The lowest functional capability or performance level of equipment required for safe operation of the facility.

Limiting Control Settings (LCS). The settings for automatic alarm or protection devices related to those variables having significant safety functions.

Margin of Safety. The level of confidence that is assigned to the integrity of radiological control measures such as confinement barriers. It is defined as the range between the design acceptance limits and the design failure point of the control feature. The design acceptance limits for radiological control measures such as confinement barriers are established during the design of the facility. These criteria are given in terms of those physical parameters that define their performance. Whenever the values of the design acceptance limits are exceeded, the margin of safety, and therefore the confidence in the integrity of the control feature, is decreased.

Normal Operation. Steady-state operation and those departures from steady-state operation that are expected frequently or regularly in the course of facility operation, system testing, and maintenance. It includes conditions such as startup, shutdown, standby, anticipated operational occurrences, operation with specific equipment out of service as permitted by the approved operational constraints, and routine inspection, testing, and maintenance of components and systems during any of these conditions if it is consistent with the approved operational constraints.

Off-site. The area outside the perimeter of the Hanford Site.

On-site. The area within the Hanford Site control perimeter, which is under the jurisdiction of DOE.

Oversight Safety Determination. The oversight of the Contractors performed by the Regulatory Unit to ensure continuing compliance to an authorization agreement.

Postulated Accidents. Events, including the design-basis events, that would have an adverse affect on the facility process but which do not have a significant probability of occurrence during the life of the facility and include, but are not limited to, pipe or tank failures.

Preliminary Safety Evaluation Report. The document, approved and issued by the Director of the Regulatory Unit, that addresses the adequacy of the authorization basis for construction.

Process. Any activity involving a highly hazardous chemical including use, storage, manufacturing, handling, or the on-site movement of such chemicals, or a combination of these activities.

Process Manager (PM). A person, designated by the Contractor Representative, responsible for ensuring that the Process Steps are accomplished.

Process Management Team (PMT). A group of individuals designated by the Contractor Representative to approve specified actions proposed by the Process Manager and to monitor their implementation.

Process Safety. The operation of facilities that handle, use, process, or store hazardous materials in a manner free of episodic or catastrophic incidents. However, the handling, use, processing, and storage of materials with inherent hazardous properties can never be done in the total absence of risk. Process safety is an ideal condition towards which one strives.

Process Safety Management. The application of management systems to the identification, understanding, and control of process hazards to prevent process-related injuries and incidents.

Public. Individuals who are not occupationally engaged at the Hanford Site.

Radiation Worker. A worker who has qualifications and training to work in a restricted area of the facility where radiation or radioactive material is present.

Regulatory Unit. The organization reporting to the Director of the Regulatory Unit dedicated to supporting the Director in executing regulatory authority.

Reliability Targets. Quantified probabilistic expectations that a component, equipment, or system will perform its intended function satisfactorily under given circumstances, such as environmental conditions, limitations as to operation time, and frequency and thoroughness of maintenance for a specified period of time. Identified important to safety items are expected to perform their function satisfactorily through all design basis accident conditions.

Requirements. Standards that are mandated by an authority through statute, regulation, or contract.

Restricted Area. An area identified by the Contractor to which access is limited for the purposes of protecting individuals against undue risk from exposure to radiation and radioactive materials. Only a radiation worker is allowed into this area.

Risk Analysis. The development of a qualitative or quantitative estimate of risk based on engineering evaluation and techniques for considering estimates of incident consequences and frequency.

Safe State. A situation in which the facility process has been rendered safe and no pressurized material flow occurs in the process lines. Any active, energy generating, process reactions are in controlled or passive equipment. The structures, systems, and components necessary to reach and maintain this condition are functioning in a stable manner, with all process parameters within normal safe state ranges.

Safety Analysis Report (SAR). A document that fully describes the analyzed safety basis for the facility (safety envelope), fully demonstrates that the facility will perform and will be operated such that radiological, nuclear, and process safety requirements are met, and fully demonstrates adequate protection of the public, the workers, and the environment.

Safety Assurance. Established confidence that adequate protection of worker and public health and safety has been provided.

Safety Basis. The combination of information relating to the control of hazards at a nuclear facility (including design, engineering analyses, and administrative controls) upon which the Director of the Regulatory Unit depends for its conclusion that activities at the facility can be conducted safely.

Safety Function. Any function that is necessary to ensure: 1) the integrity of the boundaries retaining the radioactive materials; 2) the capability to place and maintain the facility in a safe state; or 3) the capability to prevent or mitigate the consequences of facility conditions that could result in radiological exposures to the general public or workers in excess of appropriate limits.

Safety Limits. Limits on process variables associated with those physical barriers, generally passive, that are necessary for the intended facility safety functions and that are found to be required to prevent release of unacceptable levels of radioactive material to workers or the general public.

Safety Requirements Document (SRD). A document that contains the approved and mandated set of radiological, nuclear, and process safety standards and requirements which, if implemented, provides adequate protection of workers, the public, and the environment against the hazards associated with the operation of the Contractor's facilities.

Safety Requirements Document Evaluation Report. The document approved and issued by the Director of the Regulatory Unit that addresses the adequacy of the set of radiological, nuclear, and process safety standards that a Contractor proposes to implement to ensure adequate protection of worker and public health and safety.

Safety Setpoints. Physical parameters set in the control equipment by an operator for equipment that controls the process or process flow to maintain the process within the systems design safety limits. A safety set-point represents a process characteristic, such as pressure, temperature, or material level, that is monitored by a control system to restrict the process characteristic within a system's design operating range. These set-points, identified in the design as levels above which a process physical parameter would exceed a design operating range of a process component or system leading to its failure and risk to the safety of the worker, public, or the environment. Several may be used to initiate alarm levels or control the process to a safe state.

Significantly New Safety Information. Either: 1) a safety requirement newly mandated by the Regulatory Unit; 2) a safety item newly identified by the Contractor as an item not included in the SAR for the facility; or 3) a determination that an unresolved safety question exists.

Stakeholder. Any individual other than Federal employees or DOE contractor employees that will be materially affected by, or can materially affect, the outcome of the work, either favorably or unfavorably.

Standards. The expressed expectation for the performance of work.

State-of-the-Art Human Factors. The most effective design approaches established for use at the start of the final design phase.

Technical Safety Requirements. Those requirements that define the conditions, the safe boundaries, and the management or administrative controls necessary to ensure the safe operation of the facility, reduce the potential risk to the public and facility workers from uncontrolled releases of radioactive materials, and from radiation exposures due to inadvertent criticality.

Unreviewed Safety Question (USQ). A safety question where any of the following conditions are satisfied: 1) the probability of occurrence or the radiological consequences of an accident or malfunction of equipment important to safety, previously evaluated in the facility safety analyses may be increased; 2) a possibility for an accident or equipment malfunction of a different type than any evaluated previously in the facility safety analyses may be created; or 3) any margin of safety is reduced. (Also see definition for "Margin of Safety.")

Work. Functional description of a set of activities (e.g., process operations) that will produce the intended outcome or objective (such as achieving a mission in terms of specified functional requirements).

Worker. Worker means an individual within the controlled area of the facility performing work for or in conjunction with the Contractor or utilizing Contractor facilities.

Work Activities. All activities associated with performing the work, including design, construction, operation, and deactivation.

Work Activity Experts. Individuals with knowledge and expertise relevant to the work, site, and activities addressed by the standards set.